# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 13-05-2016 | FINAL | |

**4. TITLE AND SUBTITLE**

**Cyberspace at the Operational Level: Warfighting In All Five Domains**

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

**Sean Hall**

Paper Advisor: Prof John Sappenfield

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT** Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

**13. SUPPLEMENTARY NOTES** A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

**14. ABSTRACT**

Human beings have made the world a much smaller place, but mankind's propensity for violence and the nature of war have not changed. As the global population swells and resources diminish, competition between nations grows on land, on the seas, in the air, and in space. What connects all four of these domains to the people on our planet? Cyberspace, the fifth domain of warfare, is now so ubiquitous and that any military commander who ignores its potential voluntarily cedes the advantage to his enemy. This blunder may be recoverable at the tactical level, but it is catastrophic at the operational level. Potential enemies will strive to use cyberspace to deny command and control, block sustainment efforts, render fires platforms useless, falsify intelligence, deny positional awareness, and bypass force protection measures. This exploitation of cyberspace occurs with near-instantaneous speed and low risk to the initiator. Cyberspace operations can magnify effects in the other four domains and can allow an attacker to gain the initiative.

Joint Force Commanders (JFCs) and operational planners are at a crossroads. They can continue to leave the cyberspace domain to the subject matter experts, or they can foster an innovative joint force capable of planning and executing operations synchronized across all five domains in time and purpose. The clear choice is to leverage the fifth domain of warfare along with strengths in the other four domains to achieve operational objectives.

**15. SUBJECT TERMS**

**Cyberspace, domain, integration, operational art, cyber attack, cyberspace operations, information, innovation, decisive, operational objective, center of gravity, planner, commander.**

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Chairman, JMO Dept |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 24 | 19b. TELEPHONE NUMBER *(include area code)* 401-841-3556 |

**Standard Form 298 (Rev. 8-98)**

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# Cyberspace At The Operational Level: Warfighting In All Five Domains

**by**

**Sean Hall**

**Major, USAF**

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**Signature: _____**

**13 May 2016**

**Contents**

## Abstract

Human beings have made the world a much smaller place, but mankind's propensity for violence and the nature of war have not changed. As the global population swells and resources diminish, competition between nations grows on land, on the seas, in the air, and in space. What connects all four of these domains to the people on our planet? Cyberspace, the fifth domain of warfare, is now so ubiquitous that any military commander who ignores its potential voluntarily cedes the advantage to his enemy. This blunder may be recoverable at the tactical level, but it is catastrophic at the operational level. Potential enemies will strive to use cyberspace to deny command and control, block sustainment efforts, render fires platforms useless, falsify intelligence, deny positional awareness, and bypass operational protection measures. This exploitation of cyberspace occurs with near-instantaneous speed and low risk to the initiator. Cyberspace operations can magnify effects in the other four domains and can allow an attacker to gain the initiative.

Joint Force Commanders (JFCs) and operational planners are at a crossroads. They can continue to leave the cyberspace domain to the subject matter experts, or they can foster an innovative joint force capable of planning and executing operations synchronized across all five domains in time and purpose. The clear choice is to leverage the fifth domain of warfare along with strengths in the other four domains to achieve operational objectives.

## Introduction

The ability of US Department of Defense (DoD) to exploit the cyberspace domain in major operations and campaigns will be the most decisive aspect of either US victory or defeat in the next major conflict. Victors of history's wars demonstrated an ability to innovate; thereby protecting weaknesses and exploiting strengths while denying their enemy the ability to do likewise. Often, these innovations changed the character of the war through effective integration of the "new" warfighting domain of the day, whether it was sea, air, or space. Current DoD concepts of Operational Art illuminate the importance of integrating the burgeoning cyberspace domain. These concepts provide a relevant framework with which to understand cyberspace at the operational level of war. Potential enemies of the US are well aware that leveraging this domain is not an option, but a prerequisite for a successful campaign. Failure to effectively incorporate cyberspace considerations in training, planning, doctrine, and warfighting will leave DoD reeling to regain the operational and strategic initiative from those adversaries fighting in all five domains.

## Cyberspace As a Domain of Warfare

At its core, the nature of war is timeless, and inherently restricted by the bounds of human nature. Characteristics of mankind, with all their intricacies, make warfare resemble a social interaction more than art or science.[1] As such, *technology alone will never win wars*. The side that best uses the tools available to achieve relevant objectives wins. This lesson has repeated itself through history, from the Peloponnesian Wars to Operation Inherent Resolve. To paraphrase the words of Mao Tse-tung, the ability to understand the "situation

[1] Clausewitz, Carl von. *On War*. Michael Howard and Peter Paret, eds. and trans. (Princeton: Princeton University Press, 1967), 149.

as a whole" is a requisite for strategic thought one only achieves through "hard thinking."[2] Truly grasping the "situation as a whole" requires the operational planner to regard cyberspace as the warfare domain that it is, rather than to simply "sprinkle cyber" onto operational planning and execution. DoD recognized cyberspace as an operational domain in 2005, however treating cyberspace as such is still uncomfortable and difficult because it is not intuitive, and there is no playbook.[3] Innovation and critical thought are mandatory, because of our immature understanding. A look at current doctrine and the lessons of history sheds light on the formative concepts of cyberspace.

**Doctrine Reveals Immature State of Cyberspace as a Domain**

Joint Publication (JP) 5-0, Joint Operational Planning, published 11 Aug 2011, reveals an immature view of the cyberspace domain. It simply references the archaic "National Strategy to Secure Cyberspace," which was issued by the George W. Bush administration in 2003 and vaguely reminds the reader that cyberspace is part of the informational environment.[4] Thankfully, our joint force has progressed in its efforts to understand this domain within the past five years. JP 3-12, Cyberspace Operations (5 Feb 2013) clearly defines cyberspace as "a global domain within the information environment, and one of five interdependent domains, the others being the physical domains of air, land, maritime, and space."[5] This publication further describes the three layers of cyberspace as

[2] Handel, Michael I. *Masters of War: Classical Strategic Thought*. (London: Cass, 2001), 348.

[3] U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations, Joint Publication ver 2.0*. (Washington, DC: U.S. Joint Chiefs of Staff, August, 2005), 7.

[4] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operational Planning, Joint Publication JP 5-0.* (Washington DC: CJCS, 11 Aug 2011), II-10.

[5] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication 3-12*. (Washington DC: CJCS, 5 Feb 2013), v.

the *physical network* (tangible physical components), the *logical network* (programs, websites, etc.), and *cyber-persona* (people on the network).[6]

Cyberspace Operations (CO) are "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[7] This joint guidance further differentiates CO from Information Operations (IO). "CO are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace," while IO are not confined to cyberspace.[8] Although defining these terms is a necessary first step toward understanding the operating environment and tools available, truly grasping warfighting in all five domains requires much more than doctrinal definitions. History shows how well or poorly nations integrated the sea, air, and space domains in their infancy.

**History Lesson: Effectively Integrating All Available Domains Pays Dividends**

The Battle of Salamis in 480 BC, which proved to be the decisive point in the Greek-Persian war, epitomized innovation in the burgeoning domain of seapower.[9] The weaker Greek coalition used deception, geography, and maneuver to maximize the effect of their 271 triremes against the Persian fleet of more than 700 ships in support of the larger land war.[10] Prominent naval historian Julian Corbett highlights the futility of focusing too heavily on either the land or sea domain, but instead extols the advantages of "delicate interactions of the land and sea factors."[11] Corbett observes that it was *not* domination of the new domain

[6] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication 3-12*. (Washington DC: CJCS, 5 Feb 2013), v-vi.

[7] Ibid.

[8] Ibid., I-5, 6.

[9] Strause, Barry. *The Battle of Salamis: The Naval Encounter That Saved Greece—and Western Civilization*. (New York: Simon & Schuster, 2004), 3-4.

[10] Ibid., 21.

[11] Corbett, Julian S. *Some Principles of Maritime Strategy*. (London: Longmans, Green and Co, 1918), 16.

that brought victory, but innovative and effective ways to accomplish operational objectives through actions in BOTH land and sea domains.

Both World War I and World War II provide numerous examples of nations scrambling for effective warfighting methods in the fledgling domain of airspace. Early attempts to exploit advantages in the airspace domain from 1914-1918 share many parallels with military actions in cyberspace during the Gulf War in 1990-1991. World War II examples, however, are much more relevant for today's commanders and planners. For example, the ability of German forces to integrate airpower with land forces to rapidly accomplish tactical and operational objectives was a fundamental component of blitzkrieg tactics that left most of Europe promptly defeated.[12] If the Germans consolidated these operational victories under a more realistic strategy, all of Europe might be speaking German today.[13] On the other side of the English Channel, the British created the first Integrated Air Defense System (IADS) by leveraging operational level command and control and synchronizing the widespread components of airspace defense.[14] As a result, timely innovation in the young domain of airspace during the Battle of Britain brought them national survival and eventual victory in the war.

Space was the fourth domain of warfare, and strategists grappled with how to gain military advantages in this domain beginning in the early 1950s.[15] The American and Soviets launched satellites and manned space missions throughout the Cold War. Each launch validated some theories and invalidated others. Both sides sought ways to dominate

---

[12] Citino, Robert M. *The Path to Blitzkrieg: Doctrine and Training in the German Army, 1920-1939.* (London: Lynne Rienner, 1999), 244.

[13] Murray, Williamson. *Military Adaptation in War.* (Alexandria: Institute for Defense Analyses, 2009), 2-32.

[14] Ibid., 5-46.

[15] Schefter, James. *The Race: The Complete True Story of How America Beat Russia to the Moon*. (Garden City, NY: Doubleday and Co., 1999), 4-6.

the domain itself while integrating space capabilities into military operations in other domains. Ultimately, the US military found most of its advantages through communications, data for position and timing (GPS), weather, missile launch warning and tracking, reconnaissance and surveillance. Over the past few years, these critical strengths in the space domain have played an increasingly vital role in supporting military forces on land, at sea, and in the air. Although fighting wars solely in space proved both impractical and cost-prohibitive, the US has steadily acquired space capabilities that *support* military operations in other domains. As the understanding of the space domain continued simultaneously with conflict around the globe, space capabilities were refined to better support operational objectives in both planning and combat.

Space is still a very young domain in war. Civilian companies have just recently begun to rival military capabilities in space.[16] Thus far, state-sponsored militaries have endeavored to leverage space to increase the effectiveness of military operations in other domains. This "supporting domain" model is not feasible when deciding how to support operational objectives through the fifth domain of cyberspace.

As a domain, cyberspace is in many ways the antithesis of space. While space technology is expensive and exclusive, cyberspace capabilities and connections are everywhere. While innovation in space is possible through the imagination of a relative few, the talent pool for cyber capability is expanding rapidly. Reliance on cyberspace for military operations continues to grow exponentially. As a result, most nations possess a very long list of critical vulnerabilities.

[16] Fernholz, Tim, "The science behind SpaceX's ambitious plan to land a spacecraft on Mars," *Quartz,* (May 1, 2016, http://qz.com/656025/how-spacex-is-really-bringing-us-closer-to-mars-no-really/), 1.

**Recent Use of Cyberspace at Operational Level of War**

Several military operations within the past few years illustrate how effective use of cyberspace in support of operational objectives can yield rapid success with reduced risk and cost. One prime example is Russia's rapid annexation of Ukraine in February 2014. This operation leaned heavily upon informational and military instruments of national power, and they were well synchronized throughout the operation. The Russians' most notable cyberspace operations included denial, propaganda, espionage, and geolocation of enemy forces, each of which directly supported their operational objectives.[17] Despite being touted as a model of cyberspace integration into military operations, however, many experts assess that Russia utilized only a small portion of their true capability in the domain.[18]

Another example is "Israel's reported cyber attack against air defenses during a 2007 strike on a Syrian nuclear weapons facility."[19] As the Israeli jets crossed the Syrian border and proceeded to their targets, "Syrian radar screens did not show the incoming Israeli aircraft because an Israeli cyber attack had taken control of the systems, enabling the fighters to arrive undetected."[20] These are just two of many examples of effective integration of the cyberspace domain in support of operations in other domains. In the first case, the objective was political; in the second, it was military. Each new application of cyberspace capability in a major operation illustrates the immense potential of this domain. Some reports stated that the US declined to initiate military operations in Libya on March 19th, 2001, with a cyber

[17] Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (NATO CCD COE Publications: Tallinn, 2015), 11.

[18] Ibid., 9.

[19] Rice, Jonathan C, "Core Questions for Cyber Attack Guidance," *Joint Force Quarterly* 71, (2013): 33.

[20] Ibid.

attack, so as to preserve the element of surprise for future operations.[21] Was it a technical capability such as a worm or Trojan, or was it an innovative combination of basic computer network attack synchronized with actions in other domains for synergistic effects. Regardless of the reason, *ideas* are increasingly becoming the most valuable capital in this emergent domain.

The JFC or operational planner must ask, what else is possible? What capabilities are not exploited, and what vulnerabilities are not protected? Incorporating the cyberspace domain into all aspects of operational planning and execution is no longer an option; it is essential. Failure to do so will jeopardize future military operations. Many combatant commanders and joint operational planners have known this for years, and this awareness is gradually permeating the DoD. In fact, Secretary of Defense Ash Carter is currently considering elevating US Cyber Command (USCYBERCOM)to a Combatant Command.[22] The recent rush to increase "cyberspace awareness" across the services is a necessary first step in the right direction, but only one of many steps toward the modern joint force our nation requires. The potential for great gain or loss in cyberspace is so significant that all current and future joint force commanders and planners must confront this challenge and turn it into an opportunity. Fortunately, the principles of operational art provide an exceptional framework for understanding and incorporating cyberspace in major operations and campaigns.

---

[21] Manzo, Vincent, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?," *Joint Force Quarterly* 66 (2012), 9.

[22] Tucker, Patrick, "Carter May Elevate CYBERCOM to a Full Combatant Command," *Defense One*, (April 5, 2016, http://www.defenseone.com/technology/2016/04/carter-may-elevate-cybercom-full-combatant-command/127243/), 1.

## Cyberspace and Operational Art

The Principles of Operational Art underscore the imperative of visualizing the operational environment in all five domains. Operational factors, operational functions, the center of gravity, and the operational idea are only relevant to planners and commanders if they include all domains. Consequently, carefully considering the unique attributes of cyberspace is a requisite for effective integration of this domain at the operational level of war.

### Operational Factors

For over two millennia, military leaders have not only understood, but also documented the significance of time, space, and force in relation to achieving the objective.[23] In the art of warfare, balancing these *operational factors* against a military objective is critical. Proper balancing results in freedom of action at the appropriate level of war: tactical, operational, and strategic, respectively.[24] Freedom of action means retaining the initiative and forcing one's enemy to react to the character of the war rather than dictate it. Similarly, ability to disrupt the enemy's balance of operational factors can prove as advantageous as maintaining one's own balance. Understanding cyberspace at the operational level of war requires a reexamination of the traditional understanding of these factors.

### Space

While the interaction between people and machines in cyberspace requires devices located in physical spaces, our world has grown so connected that cyberspace is a seemingly infinite domain. Land, sea, air and space have clearly defined physical boundaries. As

[23] Vego, Milan. *Joint Operational Warfare: Theory and Practice.* (Newport, RI: Naval War College Press, 2009), III-3.

[24] Ibid., III-3.

mentioned in JP 3-12, the *physical network* of cyberspace comprises just one of its three layers.[25] The unique aspects of the *logical network* and *cyber persona* are what make cyberspace boundless, and more difficult to conceptualize.

Potential for damage in physical space solely initiated through cyberspace increases along with increased automation worldwide. For example, the Stuxnet virus targeted Iran's nuclear centrifuges in 2010, using programmable logic controllers to cause physical damage to those centrifuges.[26] Another increasingly important aspect of factor space is "human space." In recent conflicts, information operations in cyberspace have targeted people all over the world with propaganda in the form of videos, Tweets, posts, emails, and newsletters with unprecedented speed, volume, and in many cases, precision. Conversely, the Central Intelligence Agency uses data mining companies to monitor social media such as Twitter to gain early warning of political unrest, crises, or other factors affecting the human space.[27]

**Time**

Cyberspace has profoundly impacted the understanding of the factor time in warfare. A precious commodity during war that cannot be regained once lost, time is balanced with the other factors to achieve operational objectives. Actions in cyberspace can be nearly simultaneous, allowing prudent commanders to optimize force and space by leveraging this domain in support of actions in the other domains. Conversely, protecting one's vulnerability from enemy actions in cyberspace will help commanders avoid delays that will manifest themselves by adversely impacting force and space in the other four domains. For

[25] U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication 3-12*. (Washington DC: CJCS, 5 Feb 2013), v-vi.

[26] Milevsk, Lukas, "Stuxnet and Strategy: A Special Operation in Cyberspace?," *Joint Force Quarterly* 63 (2011), 65.

[27] Maremont, Mark and Christopher S. Stewart, "Twitter Bars Intelligence Agencies From Using Analytics Service," *The Wall Street Journal*, (May 8, 2016, http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682), 1.

example, a deception operation such as the Israel-Syria operation caused such a delay that Syria was left unable to respond, and therefore never threatened the Israeli fighters.

**Force**

Cyberspace directly or indirectly touches the operational factor of force in every modern military. Command-and-control, communications, weapons employment, navigation, and many other critical areas have grown increasingly reliant on cyberspace. When unopposed in cyberspace, *forces* react in much less *time* and cover larger *spaces*, but DoD can expect a near-peer adversary to exploit the same benefits. The ability to conceive ways to utilize cyberspace along with capabilities in other domains to adversely impact an enemy in the areas of time, space and force is precisely the innovation our joint force needs.

**Operational Functions**

Synchronizing operational functions is critical to successful operational command. Actions in cyberspace can influence operational functions to a staggering degree. In the past twenty years, technical advances in cyberspace have significantly improved DoD efficiency, effectiveness, and overall capability across the six operational functions. With this increase in capability, all services have grown heavily reliant upon cyberspace.

Operational functions such as sustainment, fires, intelligence, maneuver, and force protection provide nearly unlimited targetable nodes in cyberspace. A hacker could deny supply vessels' navigation systems, thereby delaying or preventing a critical fleet resupply mission. Corrupt software introduced to an entire squadron of bombers could render their weapons systems useless for weeks. Furthermore, cyberspace is not just an enabling domain for non-kinetic fires; it often serves their entire means of delivery, with follow-on effects realized in other domains. Falsified intelligence injected through cyberspace can lead a

theater commander to make a decision detrimental to the campaign. Ballistic missile defense missiles could be denied launch by exploiting a fire control measure. Operational movements could be delayed theater-wide through manipulation of the Time-Phased Force Deployment Data (TPFDD) system.

No operational function is more reliant on cyberspace than command and control (C2). While US military doctrine touts mission command and centralized control with decentralized execution, the campaigns of the past fifteen years have all pushed DoD organizations toward centralized execution simply because it has been possible. Near-real-time battlefield and targeting information coupled with redundant over-the-horizon communications made it unnecessary to delegate responsibility down the chain. Now, the DoD is so reliant on operational-level C2 systems that execution without them is unthinkable and rarely even practiced in training. Numerous targets and the promise of compounding effects is what makes targeting operational-level C2 nodes so desirable to our enemies. Even targeting the "seams" between our services operating in a joint operation can yield extensive results, as some level of confusion and dissonance often surrounds these seams. In short, operational functions residing in any domain can be disrupted or denied through the cyberspace domain. Operational commanders and planners must protect their own cyberspace vulnerabilities while simultaneously exploiting the critical cyberspace nodes of their adversary.

**Center of Gravity**

Another relevant concept in Operational Art is the Center of Gravity (COG). Examples of potential centers of gravity could include the national will to fight, military-industrial capability, ideology, political leadership, and fielded forces, to name a few.

Interestingly, these examples have little in common at first glance. Due to the networked world of the twenty-first century, however, all nations rely very heavily on cyberspace to assist sustainment operations during wartime. This reliance and ubiquity mean that cyberspace operations can target *any center of gravity*. This newfound opportunity for access is significant. Many historical examples illustrate that naval, air, and space operations *could not influence an enemy COG* due to its nature and domain. Today, any COG has associated vulnerabilities that adversaries can exploit through cyberspace. Cyberspace operations can prove advantageous because the entire concept of center of gravity revolves around using sources of power in the quickest and most effective way to accomplish a given political or military objective.[28]

The US joint force has been slow to recognize this potential for rapid access to the COG, despite its potential for a profound change in the character of war. In the past, near-peer belligerents were more tempted to attack each other's critical weaknesses due to stalemate or inability to attack the COG directly. Now, savvy military planners can use cyberspace to turn a critical strength into a critical vulnerability with lines of code. For example, a state-sponsored hacker could infiltrate a political leader's computer network to incriminate him or her in a controversy that could eventually lead to a criminal investigation or make it difficult to perform his/her duties adequately. The attacked nation in this example has the additional challenge of not recognizing that it lacked sufficient protection to its COG. The weakness was unknown until it was far too late to negate the effects. In the more established domains of land, sea, air, and space, "surprises" of this magnitude are far less common due to relatively linear advancement and fixed expectations.

[28] Vego, Milan. *Joint Operational Warfare: Theory and Practice.* (Newport, RI: Naval War College Press, 2009), VII-13

**Operational Idea**

The operational idea is typically "developed during the operational commander's estimate of the situation" and refined throughout the planning process.[29] It is the backbone of the operational design and is therefore hopelessly doomed to irrelevance if cyberspace potential is not optimized. Great operational ideas of history have been innovative and bold. As mentioned before, due to the nature of cyberspace, no other domain can approach its potential for innovation. Effectively synchronizing actions across multiple domains will likely enable the operational idea to take a bold approach. Furthermore, the operational commander and the operational planning team (OPT) lead do not need to be experts in cyberspace, but they must foster an environment that sees the entire situation in all five domains. For example, based upon his understanding of the situation, Commander, USPACOM, might direct his OPT to strive to incorporate operational pauses, regeneration of combat potential, operational maneuver and fires, operational deception, and the selected principles of war of offensive, maneuver, and economy of force. The key to leveraging cyberspace at the operational level occurs during the Mission Analysis and COA Development steps in the Joint Operational Planning Process (JOPP). Rather than immediately falling back to what has been done in the past, the OPT must focus on innovative ways to achieve intermediate objectives to support the operational objectives.

In the above example, the OPT might determine that the initial phase of the campaign would require offensive actions against enemy coastal defense in certain areas in able to establish local sea control. This concept may leverage the principle of maneuver and the element of operational deception by using a known weak point in cyberspace communications to transmit false navigation orders for the purpose of enemy exploitation

[29] Ibid., IX-103

and diversion of enemy surface combatants. This delay could enable blue forces to establish local sea control. They could maintain the initiative through offensive kinetic and non-kinetic operations against the enemy forces on their homeland. In conjunction with information operations initiated in cyberspace, this could provide a pathway to the COG (national will, in this case). Next, to include operational pauses for regenerating combat power after 7-10 days of fighting, the OPT might incorporate a cyber attack to degrade enemy long range maritime radar systems or their operational command and control communications. In summary, commanders and OPT leads should encourage innovation and creativity in cyberspace by clearly stating the desired effects for objective accomplishment during the Mission Analysis and COA Development phases of the JOPP.

## The Enemy Will Exploit Cyberspace

The US DoD does not have a monopoly on Operational Art. Commanders and planners who can objectively conduct a net assessment of themselves and their potential enemies place themselves on similar ground in the domain of cyberspace. The nation that spends more money on network protection will not necessarily win, and therefore cannot dwell in complacency while planning to fight wars in just four domains. In fact, any would-be adversary of the United States seeking operational effects against the US *without leveraging cyberspace* would be reckless and unwise. It is best that operational commanders and planners envision volumes of enemy plans currently on shelves today that seek to turn our critical strengths into critical vulnerabilities through Trojans, viruses, and worms.

### Inexpensive Investment in Military Capability

The number one reason why our military can expect this approach is that it is by far the least expensive way to improve one's military capability. For a nation with limited

resources, leveraging cyberspace might be the only chance to strike an effective blow against the US. Even wealthy nations recognize a need to increase investment in a cyberspace capability: not infrastructure and technology, but in manpower and their innovative potential. For example, China openly acknowledges its urgent rush to achieve operational synchronization by placing cyber forces on equal footing with military forces in other domains.[30] Russia has already demonstrated its ability to synchronize cyberspace effects with military operations and other national instruments of power to achieve operational objectives. A nation can hire or train hackers by the hundreds with the single task of locating seams in the DoD network to exploit them in the near term, or to attack them during military operations at a later date. Likewise, a similar force or portion of it could locate and eliminate seams in their own network to maintain freedom of movement in cyberspace. Investment in other domains of warfare will not yield the same results. Adding a 5% or 10% capability in the sea, land, air, or space domain is simply not as advantageous as increasing one's capability in cyberspace, which could hamper US capabilities by at least 10% in all domains. Much like Google and Apple have found ways to harness the innovation of their people, America's potential adversaries will use the relatively level playing field of cyberspace to maximize the effects of innovative ideas.

**Low Risk with Potentially High Reward**

Selected use of the cyberspace domain can mitigate risk to force and risk to the mission. State-sponsored hackers can target critical nodes in the DoD network nearly instantaneously from any location in the world. This fact makes these hackers more difficult

[30] Colley, Steven, Anthony H. Cordesman and Michael Wang. *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis*. (Washington DC, Center for Strategic & International Studies Burke Chair in Strategy: 2015), 122.

to locate, and can give the sponsor state the option to deny affiliation with any cyberspace operations against the US. When synchronized with actions in other domains, an adversary's cyberspace operations against US DoD can significantly reduce risk to their forces because they are less reliant on traditional kinetic engagements to achieve objectives. Attacking vulnerabilities within each of the operational functions will not only seize the operational initiative but can also severely impact our ability to react in a dynamic operational environment.

**Cyberspace allows an adversary to offset US strengths**

No military commander seeks to fight a war on a level playing field. Even young David knew to keep his distance from Goliath, seize the initiative, and use a standoff weapon. Potential adversaries of the US spend much time and effort determining how to offset conventional US military power. In the domain of cyberspace, this amounts to searching for "chinks in our armor." Once located, the enemy can exploit these "chinks" in the near term or short term, depending on their military objectives.

As a "status-quo" power, our nation is struggling to protect a domain so vast that it is difficult to comprehend. While senior leaders rush to integrate and consolidate stovepiped cyberspace expertise scattered across DoD, our potential adversaries have the luxury of targeting probing for and exploiting vulnerabilities with custom-made cyber forces. A small-scale cyber attack from Russia might simply serve to gauge time and scope of response from DoD, or even to assess our ability and willingness to attribute that attack to Russia. Iran might launch a similar attack simply to observe which agency responds, and improve their understanding of US authorities in cyberspace. Even more concerning, an adversary might simply introduce a virus or Trojan, affecting Fifth Fleet command and control systems, to

severely degrade or slow an operational or tactical commander's ability to make decisions. With 30,000,000 cyber attacks against DoD each year, it is a stark reminder that approximately 1,500 attacks will occur in the time it takes to read this paper.[31] Statistically, one or two of these 1,500 attacks will be successful.[32] The US will suffer from some of these effects in the short term, and others will remain concealed until a later date.

An unbiased net assessment would force any adversary to meet certain conditions to make their objectives achievable. For example, much like our military might need to attain sea control in a geographic area before follow-on operations, denying the US freedom of movement in a finite portion of cyberspace for a specified time, might allow the enemy to degrade US kinetic capability by 50%. Turning US military critical strengths into critical vulnerabilities and then rapidly exploiting advantages through actions in other domains is the best way to offset DoD strengths.

**Alternative Views**

Critics argue that actions in cyberspace will not be the most decisive aspect of US victory or defeat in the next major conflict. They assert that cyberspace will not be effectively integrated at the operational level of war due to practical limitations and overall difficulty. Others liken the supporting role of space in military operations to that of cyberspace. These critics contend that DoD network protection is important, but cyberspace operations will not play a decisive role in our next major conflict.

**Rebuttal**

These views are commonplace but seriously errant. Although integrating the fifth domain is indeed difficult, it is absolutely necessary. China, Russia, Iran and North Korea

[31] U.S. Department of Defense. DoD Cyberspace Culture and Compliance Initiative (Washington, DC: 2015), 1.

[32] Ibid.

are rapidly experimenting with better ways to integrate cyber forces and their effects throughout the range of military operations. Whether DoD is concerned with dominating shaping operations, initial phases, decisive operations, or stability operations, our adversaries will surely use all five domains to progress toward their operational objectives. Commanders and operational planners, therefore, must integrate offensive cyberspace operations with actions in other domains to best achieve objectives.

## Conclusion

In the fifth century before Christ, Spartan warriors and their slaves meticulously surveyed their armor between battles, searching for chinks or other weaknesses that would make them more vulnerable in combat. The vulnerability of one man in the Phalanx greatly reduced the effectiveness of the entire formation, and in effect, the army on the field. The US has a chink in its armor, a weakness that could adversely affect the accomplishment of its operational objectives in war. History demonstrates that the operational planners who can best think and plan operations in all domains will gain a significant advantage over their opponent. Operational Art concepts remain the primary tool for integrating cyberspace operations in support of campaign objectives. Any military force planning for conflict with the US will leverage cyberspace out of sheer necessity, if not common sense.

Integrating cyberspace with other domains is the challenge of this generation of warfighters. Innovation now will pay dividends later. Ultimately, the ability to exploit cyberspace in major operations and campaigns will be the most decisive aspect of either US victory or defeat in the next major conflict.

## Recommendations

Senior leaders across DoD are taking steps in the right direction, but they must increase their pace. The US military will only excel in cyberspace integration if manning, equipment and training allow it. Additionally, operational commanders and planners must use their positions to aggressively advance awareness of the vast potential of the cyberspace domain.

Our cyber specialists are spread across the services as well as massed at USCYBERCOM. Numbers of cyberspace experts must increase in all areas, even at the expense of capability in other domains if required. Their innovation will ultimately yield the largest part of the return on this manpower investment. With regard to training, all operational- and high tactical-level exercises must include injects that mandate network attack, exploitation, protection, etc. This is the most optimal way to foster cyberspace awareness across the joint force. It will also highlight deficiencies in tactics, techniques, and procedures as well as equipment. Due to security limitations, only a small number of specialists can accurately assess the status of our equipment at the operational and strategic level. All senior DoD leaders must trust their council and incorporate their insight into budget decisions both inside the services and before Congress.

Implementing these changes will set the course for our DoD to maintain its military advantage at the operational level of war. Effects on land, at sea, in the air, and in space will be maximized rather than undermined. Awareness of cyberspace vulnerabilities will allow protection measures *prior* to conflict rather than discovering them after the enemy has attacked the US COG. In summary, maturing the DoD understanding of operational cyberspace integration is both urgent and essential.

## Bibliography


Citino, Robert M. *The Path to Blitzkrieg: Doctrine and Training in the German Army, 1920-1939.* London: Lynne Rienner, 1999.

Clausewitz, Carl von. *On War*. Michael Howard and Peter Paret, eds. and trans. Princeton: Princeton University Press, 1967.

Colley, Steven, Anthony H. Cordesman and Michael Wang. *Chinese Strategy and Military Modernization in 2015: A Comparative Analysis*. Washington DC, Center for Strategic & International Studies Burke Chair in Strategy: 2015.

Corbett, Julian S. *Some Principles of Maritime Strategy*. London: Longmans, Green and Co, 1918.

Fernholz, Tim, "The science behind SpaceX's ambitious plan to land a spacecraft on Mars," *Quartz,* May 1, 2016, http://qz.com/656025/how-spacex-is-really-bringing-us-closer-to-mars-no-really/.

Handel, Michael I. *Masters of War: Classical Strategic Thought*. London: Cass, 2001.

Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications: Tallinn, 2015.

Manzo, Vincent, "Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?," *Joint Force Quarterly* 66 (2012).

Maremont, Mark and Christopher S. Stewart, "Twitter Bars Intelligence Agencies From Using Analytics Service," *The Wall Street Journal,* May 8, 2016, http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

Milevsk, Lukas, "Stuxnet and Strategy: A Special Operation in Cyberspace?," *Joint Force Quarterly* 63 (2011).

Murray, Williamson. *Military Adaptation in War*. Alexandria: Institute for Defense Analyses, 2009.

Rice, Jonathan C, "Core Questions for Cyber Attack Guidance," *Joint Force Quarterly* 71, (2013).

Schefter, James. *The Race: The Complete True Story of How America Beat Russia to the Moon*. Garden City, NY: Doubleday and Co., 1999.

Strause, Barry. *The Battle of Salamis: The Naval Encounter That Saved Greece—and Western Civilization*. New York: Simon & Schuster, 2004.

Tucker, Patrick, "Carter May Elevate CYBERCOM to a Full Combatant Command," *Defense One*, April 5, 2016, http://www.defenseone.com/technology/2016/04/carter-may-elevate-cybercom-full-combatant-command/127243/.

U.S. Department of Defense. DoD Cyberspace Culture and Compliance Initiative Washington, DC: 2015.

U.S. Joint Chiefs of Staff, *Capstone Concept for Joint Operations, Joint Publication ver 2.0,* Washington, DC: U.S. Joint Chiefs of Staff, August, 2005.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Cyberspace Operations, Joint Publication 3-12*. Washington DC: CJCS, 5 Feb 2013.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operational Planning, Joint Publication JP 5-0*. Washington DC: CJCS, 11 Aug 2011.

Vego, Milan. *Joint Operational Warfare: Theory and Practice.* Newport, RI: Naval War College Press, 2009.